REMARKS

Claims 1-20 remain in this application. Claims 12 and 17 have been amended. Claims 1, 12 and 17 are independent claims.

A. Basis for Rejection of Claims

In an Office action dated May 31, 2005, claims 1-11 were rejected under 35 U.S.C. 102(e) as allegedly being unpatentable over Vaidya. Claims 12-20 were rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Vaidya in view of Anderson. In response, Applicants have amended independent claims 12 and 17. Claim 12 has been amended to describe the counting of accesses for a cachable document as being collective with respect to a plurality of clients. Claim 17 has been amended to describe a file access counter as being configured such that the counting of transfers is collective.

B. Patentability of Claim 1

Claims 1-11 were rejected under 35 U.S.C. 102(e) as allegedly being unpatentable over Vaidya. Vaidya teaches (column 1, lines 18-32) that computer networks that employ a client-server model allow client devices to access resources necessary to perform functions from the servers. Vaidya also teaches that network objects may be considered to include network files (column 5, lines 57-60) and that network objects are assigned a set of attack signature profiles (column 6, lines 3-4). Attack signature profile types can be (column 7, lines 2-4) simple, sequential or time/counter based. Two types of the attack signature profiles (column 7, lines 46-49), sequential and timer/counter based, require sequential execution of an instruction or instructions. The sequential attack signature profiles (Vaidya: column 7, lines 52-67) include multiple expressions. For instance, these expressions might include "Is source address user Z?" and "Is user Z attempting to access file A?". Instructions associated with the first expression are executed on a first packet associated with an application session and a subsequent packet is analyzed to determine if user Z is attempting to access file A.

The Office action has interpreted the instructions associated with expressions for determining if a user Z source address or if user Z is attempting to access a file as being analogous to sending a network file to a

requesting device in response to a request, including an instruction to transmit an indicator subsequent to the requesting device receiving the network file. Applicants respectfully disagree. Vaidya teaches (column 5, lines 33-36) that the attack signature profiles are adapted for determining network data patterns associated with network intrusions which include unauthorized attempts to access network objects. It is submitted that an attempt to access a network object is analogous to receiving a request for a network object, not to sending a network file to the requesting device in response to the attempt.

Vaidya teaches (column 6, lines 11-14) that the attack signature profiles include a set of instructions which the virtual processor executes to determine whether a particular data packet is associated with a network intrusion. The data packet arrives during an attempt to access a network object (attempted delivery of malicious data packets capable of causing malfunction in a network object, Vaidya: column 6, lines 37-39). Therefore, the instruction being executed by the virtual processor occurs during an attempt or request for access to a network file, not an instruction included with a network file sent to a requesting device.

Furthermore, if the virtual processor (Vaidya: column 6, lines 18-25) determines that a network intrusion has occurred, it alerts a reaction module. The reaction module can either terminate the application session, trace the session or alert the network administrator of the attack. It is submitted that if the application session is terminated, the attempt to access a network object (receive a request for a network file) is also terminated. Therefore, sending a network file to a requesting device in response to the request (attempt to access) would never occur. It follows that including an instruction to transmit an indicator subsequent to the requesting device receiving the network file also would not occur.

The Office action also cited Vaidya, column 8, lines 16-39, as teaching Applicants' step of transmitting an indicator from the requesting device in response to receiving a network file. The portion of the cited reference refers to the timer/counter based signature profile which directs the virtual processor to execute instructions. The instructions direct the virtual processor to determine whether the number of attempts by user Z to access file A exceeds a preselected threshold, such as five attempts within any ten minute period. Upon recognizing the first occurrence of the particular event (e.g., user Z attempts to access file A), a timer is activated and a counter is set to "one." Each subsequent detection of the event triggers processing to

determine whether the threshold has been met within the given time. If yes, a network intrusion has been detected.

In the method described in Applicants' pending claim 1, there is a "requesting device,"

(1) from which the request for the network file is received;

(2) to which the network file is transmitted,

(3) to which an instruction is included with the network file, wherein the instruction is to transmit an indicator subsequent to receiving the network file; and

(4) from which the indicator is transmitted in response to receiving the network file.

It is respectfully asserted that the rejection of claim 1 does not present a *prima facie* case for a "receiving device" that meets these four criteria. In the rejection, the client devices (column 1, lines 18-32) are identified as the receiving devices, but the "instructions associated with file A" are clearly not included with the network file transmitted to the client devices. Instead, the "instructions" are included within the signature profiles that are stored in the signature profile memory 39. Moreover, the "indicator" that is identified in the rejection of claim 1 is not transmitted from the client/"receiving" devices of Vaidya. Rather, the triggering and counting of column 8, lines 16-39, in Vaidya occur at the data collectors that protect the client/"receiving" devices and the notifying is with respect to the reaction module 38 of the triggering/counting data collector.

It is respectfully asserted that the teachings of Vaidya do not establish a *prima facie* case of anticipation with respect to claim 1. Reconsideration of independent claim 1 and its dependent claims is requested.

C. Patentability of Claim 12-16

The Office action rejected claim 12 as allegedly being unpatentable over Vaidya in view of Anderson. Specifically, it is alleged that the combined references would teach receiving count-inducing messages transmitted from clients as responses to executable code as described by Applicants' claimed invention. In response, Applicants have amended independent claim 12 to further distinguish the claimed invention from the prior art references. The amended claim describes a method of counting a number of accesses for cachable documents comprising counting the

accesses on a basis of receiving count-inducing messages, the counting of the accesses being collective with respect to a plurality of clients. Support for the amendment resides in Paragraph [0031] of the specification as originally filed, wherein the indicator is counted for updating a tally of a total number of hits for the requested file. Moreover, Paragraph [0021] states that each count is specific to the requested file, rather than to the requesting device.

In the rejection of claim 12, it is asserted that Vaidya teaches counting accesses on the basis of receiving count-inducing messages. Specifically, column 9, lines 3-20 of Vaidya are cited. This portion of the patent relates to operations which occur for a single application session between a particular server and a particular client. Timer/counter information for the single application session is used to determine whether a network intrusion is associated with a packet. For example, the session entry might reflect that within the application session, a particular file within the application has been accessed ten times in the past twenty minutes. Greater detail regarding the timer/counter information is found in column 8, lines 16-39 of the patent. When the instructions of an attack signature profile result in a processor recognizing a first packet as being associated with a particular user attempting to access a particular file, the timer is activated and the counter is set to one. The timer and counter information is entered into a state cache. Each subsequent detection of an attempt by the same user to access the same file triggers the processor to access the timer and counter information from the state cache and to determine whether a threshold has been met. If the threshold is met, a network intrusion has been detected.

Thus, the "counting" of Vaidya is fundamentally different than the counting step described in amended claim 12. In fact, Applicants respectfully assert that if the counting as described in Vaidya were collective with respect to accesses by a plurality of clients, the Vaidya method would not work for its intended purposes. It is well settled that a modification of a prior art method or device which would render the method or device unworkable for its intended purposes cannot be said to be obvious under Section 103. Ex parte Weber, 154 USPQ 491 (P.O.Bd.Ap. 1967).

Claim 12 includes a step of embedding executable code within each of a plurality of cachable documents, wherein the executable code is associated with triggering transmissions of count-inducing messages from clients. The Office action cites column 7, line 52 to column 8, line 39 of Vaidya for teaching instructions associated with file A. However, the instructions of Vaidya are "embedded" within the attack signature profiles for

detecting network intrusions. The instructions are not embedded within cachable documents which are sent from clients in response to requests from the clients. Equally importantly, the instructions within the attack signature profiles are not associated with triggering transmissions of count-inducing messages from the clients.

In claim 12, the count-inducing messages are transmitted from the clients as responses to execution of the executable code upon reception of the cachable documents. The counting of the accesses is on the basis of receiving the count-inducing messages. Thus, it is clear from claim 12 that the count-inducing messages are generated and transmitted after the cachable documents are received by the client. In contrast, Vaidya counts requests for files. Nothing within the Vaidya patent would render it obvious to fundamentally modify its intrusion-detection techniques to count file accesses after the files have been exchanged.

The Office action correctly notes that Vaidya does not explicitly detail "receiving said count-inducing messages transmitted from said clients as responses to said executable code." Therefore, the last paragraph in column 3 and the first paragraph in column 4 of Anderson are cited. Applicants respectfully point out that, like Vaidya, the process sequencing is fundamentally different than the sequence described in claim 12. Anderson teaches a system for the centralized storage and management of electronic messages. As described in column 3, lines 31-47, a Message Distribution Server (MDS) system receives electronic messages to be distributed to recipients. A single copy of each message is centrally stored, along with various information about sending the message. The MDS system sends a short indicator message to each recipient to notify the recipient that the electronic message is available. The MDS system then tracks and manages requests from the recipients to access the message. The indicator message sent to the recipients can take a variety of forms. For example, the indicator message can include the sender and the subject line only, the first few lines from the message body, or message attributes, such as size or importance. Each indicator message also includes a reference to the corresponding message that will allow the message to be accessed. After a recipient receives the indicator message, the recipient can use the indicator to access the centrally stored electronic message. A reference to the corresponding message in the indicator can allow the electronic message to be accessed either manually (e.g., clicking on a link, such as a URL) or automatically (e.g., retrieving the message when the indicator is selected).

Anderson was cited for its teachings regarding the indicator message sent to the recipient, to allow accessing manually or automatically, such as via a URL. However, the URL as taught by Anderson is not embedded within the cachable documents that are transmitted to the clients in response to requests from the clients. That is, the URL as taught by Anderson is not embedded within the electronic messages. Rather, the URL is contained within the indicator message that is transmitted prior to any requests for the cachable documents.

Anderson teaches embedding the URL in a message that precedes the request. The primary reference of Vaidya teaches counting requests that are necessarily prior to sending the cachable documents to the clients. It follows that even if one were to modify the primary reference of Vaidya to include selected teachings of Anderson, the resulting method would not render claim 12 obvious under Section 103(a).

Reconsideration of independent claim 12 and its dependent claims is requested.

D. Patentability of Claims 17-20

The Office action rejected independent claim 17 as allegedly being unpatentable over Vaidya in view of Anderson. In response, Applicants have amended claim 17 to more clearly distinguish the invention from the cited prior art. Specifically, the file access counter is described as being configured such that the counting is collective with respect to the transfers of the network files to the "plurality of clients." The collective counting with respect to the clients is consistent with the amendment made to independent claim 12. Consequently, many of the comments made with regard to the patentability of claim 12 apply equally to the determination of patentability of claim 17.

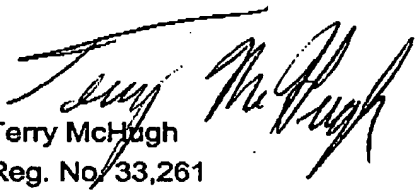
The primary reference to Vaidya does not teach or suggest a file access counter that is configured such that counting of transfers of files is collective with respect to the transfers to a plurality of clients. Rather, the counting as described in Vaidya is "user-specific." That is, a count is made as to whether a specific user has requested access to a specific file a specific number of times within a specific time period. Even if one were to modify Vaidya in view of selected teachings of Anderson, the resulting system would not teach or suggest Applicants' claimed invention.

In claim 17, the file access counter is responsive to receiving identifiers from any one of the plurality of clients as a basis for counting transfers of the network files to the clients. In Vaidya, the counting is responsive to reception of a request for a transfer. The goal in Vaidya is to detect network intrusions. The processing is fundamentally different than processing for tracking the number of "hits."

In Anderson, the URL indicator is embedded within the indicator message. This indicator message precedes the reception of requests from the clients. It necessarily follows that the indicator message precedes the transmission of the requested "network files" to the clients. Consequently, the combination of teachings of Vaidya and Anderson does not establish a *prima facie* case of obviousness under Section 103(a).

Applicants respectfully request reconsideration of the claims in view of the amendments and remarks made herein. A notice of allowance is earnestly solicited. In the case that any issues regarding this application can be resolved expeditiously via a telephone conversation, Applicants invite the Examiner to call Terry McHugh at (650) 969-8458.

Respectfully submitted,



Terry McHugh
Reg. No. 33,261

Date: August 30, 2005

Telephone: (650) 969-8458
Facsimile: (650) 969-6216